

RECEIVED
CENTRAL FAX CENTER

OCT 12 2007

100.2412
Branigan 2-10

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of : Branigan et al.
For : Methods and Apparatus for Secure Wireless
Networking
Serial No. : 09/755,470
Filed : 01/05/2001
Group : 2134
Examiner : Tran, Ellen C.

Durham, North Carolina
October 12, 2007

MAIL STOP APPEAL BRIEF – PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

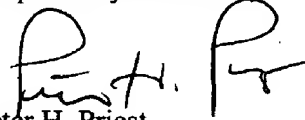
TRANSMITTAL OF APPELLANT'S BRIEF

Dear Sirs:

1. Transmitted herewith is the APPEAL BRIEF in this application with respect to the Notice of Appeal filed on July 12, 2007.
2. The Applicant is other than a small entity.
3. Pursuant to 37 CFR 1.17(f) the fee for filing the Appeal Brief is \$510.00.
☐ [x] The Commissioner is hereby authorized to charge the fee of \$510 our credit card.
☐ [x] The Commissioner is hereby authorized to charge the 1 month extension fee of \$120 to our credit card. This letter petitions for a one month extension of time.

- [] The Commissioner is hereby authorized to charge any additional fees which may be required or credit any overpayment to Law Offices of Peter H. Priest Deposit Account No. 50-1058.

Respectfully submitted,



Peter H. Priest
Reg. No. 30,210
Priest & Goldstein, PLLC
5015 Southpark Drive, Suite 230
Durham, NC 27713
(919) 806-1600

RECEIVED
CENTRAL FAX CENTER

OCT 12 2007

100.2412
Branigan 2-10

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of : Branigan et al.
For : Methods and Apparatus for Secure Wireless
Networking
Serial No. : 09/755,470
Filed : 01/05/2001
Group : 2134
Examiner : Tran, Ellen C.

10/16/2007 SSITHIB1 00000006 09755470

01 FC:1402 510.00 OP

Durham, North Carolina
October 12, 2007

MAIL STOP APPEAL BRIEF – PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF

Sir:

1. The Real Party In Interest

The real party in interest is the assignee, Lucent Technologies Inc.

2. Related Appeals and Interferences

None.

3. Status of the Claims

This is an appeal from the April 13, 2007 final rejection of claims 1-15, all of the

pending claims. Claims 1 and 7 stand rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 6,393,484 (Massarani) in view of Lewis U.S. Patent No. 6,526,506 (Lewis). Claims 2-5 and 8-13 stand rejected under 35 U.S.C. § 103(a) over Massarani in view of Lewis in further view of Bhagwat et al. U.S. Patent No. 6,651,105 (Bhagwat). Claim 6 stands rejected under 35 U.S.C. § 103(a) over Massarani in view of Redlich U.S. Patent No. 6,591,306 (Redlich). Claims 14 and 15 stand rejected under 35 U.S.C. § 103(a) over Massarani in view of Lewis in view of Bhagwat in further view of Schuster et al. U.S. Patent No. 6,857,072 (Schuster). Claims 1-15 are the subject of this appeal.

4. Status of Amendments

The claims stand as last amended on January 29, 2007. An Amendment After Final has been filed to make a change required by the final Official Action to correct an obvious typographical error and place the claim in better order for appeal.

5. Summary of Claimed Subject Matter

Among its several aspects, the present invention addresses security problems presented when wireless networks connect with wired networks. The Background of the Invention describes the problem and several prior art approaches to the problem in some detail. Page 1, line 8-page 4, line 3.

As addressed in greater detail below, according to one aspect of the invention, once a wireless network client has been authenticated, a unique session key to be used for encrypted communication with the wired network is provided. The session key is used by the client during one connection session to the wired network. Page 4, lines 17-22. An eavesdropper cannot gain access to network information because all traffic over the wireless network which contains substantive information from the wired network is encrypted. Page 5, lines 6 and 7.

Claim 1

Turning to the claims, claim 1 addresses a "wired network for providing secure, authenticated access to wireless network clients" exemplary structure and operation of which are illustrated in Figs. 1-3 and described at page 4, line 52 to page 14, line 4.

The wired network comprises "a server connected to a wireless network access point" such as the exemplary SB server 102 connected to wireless access point 112 of Fig. 1 described at page 6, lines 1-20, for example.

The server has "access to the wired network" as shown in Fig. 1 and described at page 6, lines 2 and 3, for example.

The server is "operative to perform authentication for a wireless client establishing a connection to the server through the wireless network access point," as described at page 6, lines 2-4, for example.

The server performs "authentication by examining authentication information transmitted from the client to the server and determining whether or not the authentication information identifies the wireless network client as authorized to gain access to the wired network," as described at page 7, lines 12-15, and page 9, lines 2-6, for example.

The server is further "operative to establish a connection session upon authentication of a client." Page 8, lines 1-4, and page 9, line 6-page 10, line 9, for example.

The server is "also operative to provide the client with a wired network address valid for the connection session upon authentication of the client." Page 4, lines 18-23; page 6, lines 4-8; and page 9, lines 21 and 22, for example.

The server is "further operative to encrypt communications with the wireless network access point." Page 7, lines 8-18; and page 9, line 23-page 10, line 6, for example.

The server is "further operative to provide a cryptographic key to the client to be used for encrypted communication with the wired network and valid for the connection session, upon authentication of the client." Page 4, lines 22 and 23; page 10, lines 2-4; and page 13, lines 18 and 19, for example.

The wired network also comprises "a user database accessible to the server for use in validating wireless clients," such as user authentication database 108, as described at page 6, lines 6-8, for example.

Claim 7

Claim 7 addresses a "wireless network for providing secure authenticated communication between clients of the wireless network and a wired network," exemplary structure and operation of which are shown in Figs. 1-3 and described at page 4, line 5 to page 14, line 4.

The wireless network comprises "a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network", such as wireless access point 112 of wireless network 104 which operates to establish a connection with SB server 102 and wired network 100 as described at page 6, lines 1-20, for example.

The wireless network access point "being operative to conduct communications with the server in order to authenticate wireless network clients as authorized to access the wired network." Page 8, lines 1-3, for example.

The wireless network access point "being further operative to receive authentication information from one or more wireless network clients and transfer the authentication information to the server in order to allow the server to examine the authentication information for a wireless client and determine if the information indicates that the wireless network client is

authorized to access the wired network." Page 9, lines 1-13, for example.

The wireless network access point "being further operative to receive a cryptoprocessing key valid for a connection session from the server upon authentication of a client and to transfer the cryptoprocessing key to that client." Page 9, line 21-page 10, line 9, for example.

The wireless network client is "operative to establish connections with the wireless network access point." Page 6, lines 9-15, for example.

The client "being operative to conduct encrypted communications with the wireless network access point." Page 7, lines 15-18, for example.

The client being operative "to pass authentication information to the network access point in order to indicate to a server communicating with the wireless network and a wired network whether or not the wireless client is authorized to gain access to the wired network." Page 7, lines 12-18, for example.

The wireless network client "being further operative to receive address information and the cryptoprocessing key from the network access point upon authentication by the server in order to allow communication with the wired network." Page 9, line 21-page 10, line 9, for example.

The client "utilizing the cryptoprocessing key to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and the cryptoprocessing key." Page 10, lines 4-6, for example.

Claim 10

Claim 10 addresses "a method of secure communication between wireless network clients and a wired network," for which exemplary operation and structure for supporting such operation are described at page 4, line 5 to page 14, line 4 and shown in Figs. 1-3.

The method comprises "establishing a connection between a wireless network access point and a security base (SB) server connected to the wired network." Page 12, line 21-page 13, line 4.

The method also comprises "establishing a connection between the SB server and a wireless network client communicating with the SB server through the wireless network access point." Page 13, lines 5-11, for example.

The method also comprises "exchanging encryption keys between the SB server and the wireless network client." Page 13, lines 10 and 11, for example.

The method also comprises "transmitting authentication information from the wireless network client to the SB server through the wireless network access point." Page 13, lines 11-16, for example.

The method also comprises "performing authentication for the wireless network client by examining the authentication information to determine if the wireless network client is authorized to gain access to the wired network." Page 13, lines 16 and 19, and page 9, lines 1-13, for example.

The method also comprises "if authentication fails, rejecting connection to the wired network." Page 13, lines 15 and 16, and page 9, lines 13-15, for example.

The method also comprises "if authentication passes, accepting connection to the wired network, providing a temporary wired network address and a unique session encryption key to the wireless network client for encrypted communication with the wired network and valid for the connection session and providing access to wired network resources in response to requests by the wireless network client." Page 13, lines 16-20 and page 9, line 19-page 10, line 9, for example.

6. Grounds of Rejection to be Reviewed on Appeal

Claims 1 and 7 stand rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 6,393,484 (Massarani) in view of Lewis U.S. Patent No. 6,526,506 (Lewis). Claims 2-5 and 8-13 stand rejected under 35 U.S.C. § 103(a) over Massarani in view of Lewis in further view of Bhagwat et al. U.S. Patent No. 6,651,105 (Bhagwat). Claim 6 stands rejected under 35 U.S.C. § 103(a) over Massarani in view of Redlich U.S. Patent No. 6,591,306 (Redlich). Claims 14 and 15 stand rejected under 35 U.S.C. § 103(a) over Massarani in view of Lewis in view of Bhagwat in further view of Schuster et al. U.S. Patent No. 6,857,072 (Schuster).

7. Argument

The final rejection under 35 U.S.C. § 103 did not follow M.P.E.P. § 706.02(j) which states:

After indicating that the rejection is under 35 U.S.C. 103, the Examiner should set forth...the difference or differences in the claim over the applied reference,...the proposed modification of the applied reference(s) necessary to arrive at the claimed subject matter, and ... an explanation why one of ordinary skill in the art at the time the invention was made would have been motivated to make the proposed modification.

The art rejections are based on Massarani in view of Lewis (claims 1 and 7), Massarani in view of Lewis in further view of Bhagwat (claims 2-5 and 8-13) or Massarani in view of Redlich (claim 6), or Massarani in view of Lewis in view of Bhagwat in further view of Schuster (claims 14 and 15). These art rejections are not supported by the relied upon items, and the analysis supporting those rejections is traversed in its entirety.

Claims 1 and 7

Massarani addresses a "System or Method for Controlled Access to Shared-Medium Public and Semi-Public Interest Protocol (IP) Networks." Massarani addresses how "to control

and restrict access to the networks only to authorized and registered devices and users. One example of the problem relates to corporate IP network administrators who deal with an increasingly mobile work force that have deployed IP network access ports (typically IEEE 802.X or similar medium) throughout their corporate facilities for shared use by their employees." Massarani, col. 1, lines 14-25. "A strong concern in the use of such networks is preventing visitors or unauthorized persons from taking advantage of the exposed network access ports to gain IP connectivity to the internal corporate network (intranet)." Col. 1, lines 27-30. Massarani continues with a discussion of prior art (col. 1, line 50 – col. 2, line 62) concluding, "Such systems rely on encryption and sophisticated key management system which makes such techniques expensive, inflexible, and not suitable for shared-medium public and semi-public IP networks. What is needed is a system and method that is applicable to existing and future network access infrastructures which works in conjunction with popular and established IP protocols and communication layer network equipment without requiring any modifications to currently used internet protocols." Massarani, col. 2, line 62-col. 3, line 4. As such Massarani is a very poor reference for purposes of any obviousness analysis, as--if anything--it teaches away from the presently claimed invention which addresses a design approach with a modified infrastructure based on "a wireless access point" as claimed and "a server" as claimed.

The Official Action correctly admits at pages 3 and 4 that Massarani fails to teach both "the server being further operative to encrypt communications with the wireless network access point" and "the server being further operative to provide a cryptographic key valid to the client for encrypted communication and valid for the connection session upon authentication of client". The latter part of claim 1 actually reads "the server being further operative to provide a cryptographic key to the client **to be used for encrypted communication with the wired**

network and valid for the connection session upon authentication of the client".

The final Official Action relies upon Lewis as purportedly overcoming these admitted deficiencies. As addressed in greater detail below, Lewis does not provide a basis for modifying Massarani to meet the present claims.

First, however, Massarani does not meet other elements of both claims 1 and 7, and the analyses of the Official Action at page 3, paragraph 6 (claim 1) and pages 6 and 7 (claim 7) are fundamentally flawed and incorrect.

Claim 1 addresses "a server connected to a wireless network access point, and having access to the wired network". As seen in Fig. 1 of the present application, wireless access point 112 is connected to security base (SB) server 102 which has access to and controls access to wired network 100. By contrast, Fig. 1, the sole figure of Massarani showing structural details, shows a plurality of end user devices connected to ports 10^1 to 10^N and 12^1 to 12^N . These ports are connected directly to the network 14 so that apparently an eavesdropper who has overheard a wireless communication including log in information can directly access the network 14 by simply connecting to a port and using that information.

By contrast, in the present claims, the SB server controls access to the wired network. In the words of claim 1, "the server being operative to perform authentication for a wireless client establishing a connection to the server through the wireless access point". Apparently, the Official Action relies upon DHCP server 30 or optional authentication server 36 of Massarani as performing this claimed operation and function. However, these servers are connected to the access ports through layers of edge router/switches 22^1 , 22^N , network lines 24^1 , 24^N and the edge router/switch 20^1 so that the boundary of the network 14 is not protected by these servers in the same way SB server 102 protects network 100, for example.

This difference is fundamental. The claimed invention as illustrated in Fig. 1, for example, allows no access to the network by the wireless client until that client is authenticated. Thus, there is no opportunity for the eavesdropper to bypass the SB server 102 which effectively stands guard at the door whereas the DHCP server 30 of Massarani may be viewed as inside the door and all the way across the room. The server of claim 1, like SB server 102 of Fig. 1, performs "authentication" and operates to establish a connection session "upon authentication of a client".

Thus, a client only gains access to the wired network, such as network 100, upon authentication by the SB server 102. No connection session is established absent authentication so there is no access at all to wired network 100. By contrast, in Massarani, anyone connecting to a port has immediate direct access to network 14.

Claim 1 also recites that the server provides "the client with a wired network address valid for the connection session." The final Official Action relies upon Massarani col. 4, lines 31-41 and col. 6, lines 23-53 as purportedly meeting this required limitation of the claim. However, this relied upon text clearly does not literally or inherently meet the quoted language from claim 1, and is set forth below for ease of reference:

In FIG. 1, a plurality of mobile/dynamic end user devices $10^1, \dots, 10^N; 12^1, \dots, 12^N$, etc., for example PC's, internets, smart phones, etc., are connected to a shared-medium network 14 which prevents unauthorized devices and users from obtaining network services. The devices 10, 12 are connected to the network 14 through a layered communication system, e.g., TCP/IP Open System Interconnection (OSI) using layers 2 and 3. The devices 10, 12 are connected to the network at access ports $20^1, \dots, 20^N$, typically IEEE 802.X or similar medium in which the data link layer 2 Massarani col. 4, lines 31-41

In FIG. 4, a device authentication process 400 is initiated in an operation 402 when the end user device connects to the network access port and powers on. In an operation 404, the end user device such as a PC or CM will initiate a DHCP exchange in an attempt to obtain a valid IP

address and other associated parameters. The first part of the exchange, is a MAC broadcast DHCP request for IP address, which contains in the request the end user's device MAC address.

In an operation 406, the associated edge router/switch will pick up and forward to the DHCP server 30 (see FIG. 1) the end user's devices DHCP request. At this point, no IP traffic is yet taking place between the edge router/switch and the end user device; therefore, ARP to MAC conversion is not needed. In an operation 408, the DHCP server will process the end user's device DHCP request and extract the end user's device MAC address from the database 32 (see FIG. 1).

A test 410 is performed to determine whether the MAC address is registered. A "no" condition initiates an operation 412 in which the end user's device MAC address, the DHCP server access devices and/or user information is checked in the service database 32. If the MAC address is invalid, that is, not previously registered, the DHCP server refuses to handle the request, and logs the attempt, potentially alerting network operators of a possible security breach and the process ends. If the MAC address is valid, that is belongs to a registered user, a "yes" condition for the test 410 activates the DHCP server in an operation 414, selects an appropriate IP address and associated parameters to be returned to the requesting end user device. Massarani col. 6, lines 23-53

Compare, for example, the discussion of Massarani, col. 3, lines 54-col. 4, line 8 which addresses a provisional IP lease, a timer for a suggested duration, and the statement at lines 65 and 66 that after successful authentication "the end user can be moved" which appear inconsistent with the claimed "wired network address valid for the connection session".

Returning to Lewis, Lewis like Massarani shows an arrangement in which access points serve as entrance points directly to the wired network. Lewis states in this regard "Each access point 54 serves as an entrance point through which wireless communications may occur with the system backbone 52." Thus, Lewis provides no basis for modifying Massarani in a manner so as to meet the present claims, and effectively teaches away from the present claims.

Because it lacks the infrastructure of the present claims, Lewis addresses a multi-level encryption scheme for a wireless network. Title, Abstract. A first level of encryption is provided for communications between a mobile and an access point. A second level is provided

for wireless communications distributed onto the wired system backbone. Col. 2, lines 46-52. As addressed at col. 2, lines 13-17, this two level approach is said to address problems presented as "By eavesdropping on such communications, the individual may then ascertain a system ID within the network. The individual may then proceed to place unauthorized traffic on the network using the unauthorized mobile terminal."

Claim 7 was rejected on a similar basis as claim 1, and it is allowable on the basis argued above. However, it is further noted that claim 7 focuses on details of the "wireless network access point" and specifically recites "connection with a server **operating as a portal between** the wireless network and a wired network". It does not appear that any server of Massarani or Lewis operates in such a manner, and Lewis specifically notes at col. 5, lines 7-10 that absent encryption "such eavesdropping can enable the operator of the UMT 70 to gain access to the system backbone 52 and potentially be able to place traffic onto the system backbone 52." Further, no details of the operation of access points of Massarani or Lewis meet the claimed wireless access point operation of claim 7. The Official Action's analysis of the language of claim 7 does not support a rejection of this claim.

Claims 2-5 and 8-13

Claims 2-5 and 8-13 stand rejected based on Massarani in view of Lewis in further view of Bhagwhat. In rejecting independent claim 10, the analysis of the Official Action is flawed as noted above in the discussion of Massarani and Lewis with respect to claims 1 and 7 above.

Claim 10 further recites "providing access to wired network resources in response to requests by the wireless-client" which the Official Action admits "is not explicitly taught in Massarani and Lewis relying on Bhagwhat at col. 3, lines 41-48. This portion of Bhagwhat addresses preserving an already established PPP connection during hand-offs when a mobile

moves to a new access point. This disclosure of Bhagwhat does not meet the above recited language of claim 10. The Official Action cryptically suggests "additional resources is an obvious variation of peers"; however, nothing in the cited portion of Bhagwhat suggests anything beyond a handoff in which the status quo is simply maintained. In other words, that the previous allocation of resources is maintained.

With regard to claim 2, the Official Action suggests Massarani's edge router switch meets the claimed "network hub"; however, the pertinent portion of claim 2 reads in full "a network hub providing connections between the server and additional resources of the wired network". The edge router/switches 20¹ and 22^N of Massarani do not meet the terms of claim 2. As seen in Fig. 1 of the present application, for example, network hub 106 does indeed connect SB server 102 to other resources of wired network 100. The above noted edge/router switches of Massarani only serve to connect DHCP server 30 or optional authentication server 36 to ports 10¹-10^N and 12¹ to 12^N. These ports are apparently viewed by the Official Action as access points, and as such, do not comprise resources of the wired network. If they do not comprise "access points", then this element is lacking from Massarani. This noted difference is significant because as noted above a server, such as SB server 102 of Fig. 1 of claim 1 effectively guards the door to the network 100. The claimed arrangement of the network hub of claim 2 serves to further emphasize this distinction and further distinguishes the very different structure addressed by Massarani.

As to the remaining dependent claims, the additionally relied upon items do not cure the deficiencies of Massarani and Lewis addressed above.

B. Rejections under 35 U.S.C. § 103(a)

The art rejections are not supported by the relied upon art. All of the rejections are based

on Massarani in combination with one, two or three other items. 35 U.S.C. § 103 which governs obviousness indicates that "differences between the subject matter sought to be patented and the prior art" must be assessed based upon "the subject matter as a whole". Analyzing the entirety of each claim, the rejections under 35 U.S.C. § 103 are not supported by the relied upon art as addressed further below. Only after an analysis of the individual references has been made can it then be considered whether it is fair to combine teachings. However, as addressed further below, fairness requires an analysis of failure of others, the lack of recognition of the problem, and must avoid the improper hindsight reconstruction of the present invention. Such an analysis should consider whether the modifications are actually suggested by the references rather than assuming they are obvious.

The 35 U.S.C. § 103 rejections made here pick and choose elements from at least two separate references, neither of which presents any motivation for making the suggested combination. This approach constitutes impermissible hindsight and must be avoided.

To sum up, the relied upon art does not show and does not suggest a wired network, a wireless network, and a method of providing secure communication between a wired network and a wireless network as presently claimed. Nothing in the relied upon references teaches or makes obvious a system or method which solves the problems advantageously addressed by the present invention. The claims of the present invention are not taught, are not inherent, and are not obvious in light of the art relied upon.

C. The Examiner's Findings of Obviousness are
 Also Contrary to Law of the Federal Circuit

As shown above, the invention claimed is not suggested by the relied upon prior art. The references cited by the Examiner, if anything, teach away from the present invention taking different approaches to providing secure communication. Massarani suggests that it seeks to be

compatible with existing and future infrastructures, that existing infrastructures need not be modified, and Lewis is encryption based. In both, wireless clients or access points connect directly to the wired network. Thus, it is only in hindsight, after seeing the claimed invention, that the Examiner could combine the references as the Examiner has done. This approach is improper under the law of the Federal Circuit, which has stated that “[w]hen prior art references require selective combination by the Court to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight gleaned from the invention itself.” Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051, 5 U.S.P.Q. 2d 1434, 1438 (Fed. Cir. 1988), cert. den., 109 S. Ct. 75, 102 L.Ed. 2d 51 (1988); quoting Interconnect Planning Corp. v. Feil, 774 F.2d 1132, 1132, 227 U.S.P.Q. 543, 535 (Fed. Cir. 1985). Furthermore, “[i]t is impermissible to use the claims as a frame and the prior art references as a mosaic to piece together a facsimile of the claimed invention.” Uniroyal, 837 F.2d at 1051, 5 U.S.P.Q. 2d at 1438.

In addition, the Examiner does not appear to have considered “where the references diverge and teach away from the claimed invention”, Akzo N.V. v. International Trade Commission, 808 F.2d 1471, 1481, 1 U.S.P.Q. 2d 1241, 1246 (Fed. Cir. 1986), cert. den., 107 S. Ct. 2490, 482 U.S. 909, 107 S.Ct. 2490 (1987); and W.L. Gore Associates, Inc., 721 F.2d 1540, 220 U.S.P.Q. 303 (Fed. Cir. 1983); nor has the Examiner read the claims as a whole, as required by statute. 35 U.S.C. §103. See also, Smithkline Diagnostics Inc. v. Helena Laboratories Corp., 859 F.2d 878, 885, 8 U.S.P.Q. 2d 1468, 1475 (Fed. Cir. 1988); and Interconnect Planning Corp., 774 F.2d at 1143, 227 U.S.P.Q. at 551. Here, both of the main items relied upon, namely Massarani and Lewis, show arrangements where wireless devices or wireless access points connect directly to the wired network with no intermediary server to protect the wired network

boundary.

In In re Laskowski, 871 F.2d 115, 10 U.S.P.Q. 2d 1397, the Federal Circuit reversed an obviousness rejection of the claims in an application for a bandsaw. The claimed bandsaw used a pulley type wheel loosely fitted with a tire. The primary reference showed a similar bandsaw where the band was tightly fitted. The Federal Circuit stated that the prior art did not provide a suggestion, reason or motivation to make the modification of the reference proposed by the Commissioner. Id. at 1398. The Court added that “there must be some logical reason apparent from the positive, concrete evidence of record which justifies a combination of primary and secondary references.” Id. quoting In re Regel, 526 F.2d 1399, 1403, 188 U.S.P.Q. 136, 139 (C.C.P.A. 1975), citing In re Stemniski, 444 F.2d 581, 170 U.S.P.Q. 343 (C.C.P.A. 1971).

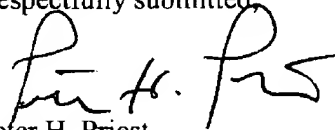
In Uniroyal Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 U.S.P.Q. 2d 1434 (Fed. Cir. 1988), cert. den., 109 S. Ct. 75, 102 L.Ed. 2d 51 (1988), the Federal Circuit reversed the District Court’s finding that the claims for a patent for an air flow deflecting shield were obvious. Without any suggestion in the art, the District Court improperly chose features from several prior art references to recreate the claimed invention.

The Examiner’s rejection suggests that the Examiner did not consider and appreciate the claims as a whole. The claims disclose a unique combination with many features and advantages not shown in the art. It appears that the Examiner has oversimplified the claims and then searched the prior art for the constituent parts. Even with the claims as a guide, however, the Examiner did not recreate the claimed invention.

8. Conclusion

The rejection of the pending claims should be reversed and the application promptly allowed.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Peter H. Priest".

Peter H. Priest
Reg. No. 30,210
Priest & Goldstein, PLLC
5015 Southpark Drive, Suite 230
Durham, NC 27713
(919) 806-1600

CLAIMS APPENDIX
(Claims Under Appeal)

1. A wired network for providing secure, authenticated access to wireless network clients, comprising:

a server connected to a wireless network access point, and having access to the wired network, the server being operative to perform authentication for a wireless client establishing a connection to the server through the wireless network access point, the server performing authentication by examining authentication information transmitted from the client to the server and determining whether or not the authentication information identifies the wireless network client as authorized to gain access to the wired network, the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client, the server being further operative to encrypt communications with the wireless network access point, the server being further operative to provide a cryptographic key to the client to be used for encrypted communication with the wired network and valid for the connection session, upon authentication of the client; and

a user database accessible to the server for use in validating wireless clients.

2. The wired network according to claim 1 and also including a network hub providing connections between the server and additional resources on the wired network.

3. The wired network according to claim 1 and also including a router providing connections between the server and additional resources on the wired network as well as a connection to an additional wired network.

4. The wired network according to claim 2 wherein the server is operative to provide

addresses to clients through dynamic host control protocol.

5. The wired network according to claim 4 wherein the server is operative to communicate with a wireless network client using point to point tunneling protocol.

6. The wired network according to claim 5 wherein the server employs 128-bit cryptoprocessing to communicate with the wireless network client.

7. A wireless network for providing secure authenticated communication between clients of the wireless network and a wired network, comprising:

a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network, the wireless network access point being operative to conduct communications with the server in order to authenticate wireless network clients as authorized to access the wired network, the wireless network access point being further operative to receive authentication information from one or more wireless network clients and transfer the authentication information to the server in order to allow the server to examine the authentication information for a wireless network client and determine if the information indicates that the wireless network client is authorized to access the wired network, the wireless network access point being further operative to receive a cryptoprocessing key valid for a connection session from the server upon authentication of a client and to transfer the cryptoprocessing key to that client; and

a wireless network clients operative to establish connections with the wireless network access point, the client being operative to conduct encrypted communications with the server through the access point, to pass authentication information to the network access point in order to indicate to a server communicating with the wireless network and a wired network whether or not the wireless client is authorized to gain access to the wired network, the wireless network

client being further operative to receive address information and the cryptoprocessing key from the network access point upon authentication by the server in order to allow communication with the wired network, the client utilizing the cryptoprocessing key to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and the cryptoprocessing key.

8. The wireless network of claim 7 wherein the access point communicates with the server using point to point tunneling protocol.

9. The wireless network of claim 8, also including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point communicating with a plurality of additional wireless network clients, the wireless network access point and the additional network access points being operative to establish connections with the server through the network hub.

10. A method of secure communication between wireless network clients and a wired network, comprising the steps of:

establishing a connection between a wireless network access point and a security base (SB) server connected to the wired network;

establishing a connection between the SB server and a wireless network client communicating with the SB server through the wireless network access point;

exchanging encryption keys between the SB server and the wireless network client;

transmitting authentication information from the wireless network client to the SB server through the wireless network access point;

performing authentication for the wireless network client by examining the authentication information to determine if the wireless network client is authorized to gain access to the wired

network;

if authentication fails, rejecting connection to the wired network; and

if authentication passes, accepting connection to the wired network, providing a temporary wired network address and a unique session encryption key to the wireless network client for encrypted communication with the wired network and valid for the connection session and providing access to wired network resources in response to requests by the wireless network client.

11. The method of claim 10 wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection and wherein the step of accepting the connection is accompanied by a step of logging the acceptance.

12. The method of claim 11 wherein the step of providing a temporary wired network address to the wireless network client includes using dynamic host control protocol to provide the address.

13. The method of claim 12 wherein communication between the wireless network client and the wired network server is performed using point to point tunneling protocol.

14. The method of claim 13 wherein the step of performing authentication for the wireless network client includes transferring authentication information between the wireless network client and the SB server and wherein the authentication information is encrypted using public key cryptography.

15. The method of claim 14 wherein the step of providing a unique session encryption key includes encrypting the unique session encryption key using public key cryptography.

EVIDENCE APPENDIX

None.

None.

RELATED PROCEEDINGS APPENDIX